Privacy Impact Assessment
Geospatial Systems (GS)

Policy, E-Government and Fair Information Practices

- Version: 1.4
- Date: 09/01/2020
- Prepared for: USDA OCIO-Policy, E-Government and Fair Information Practices (PE&F)

USDA
United States Department of Agriculture

Privacy Impact Assessment for the

Geospatial Systems (GS)

09/01/2020

Contact Point

Amy Penechar, Project Manager, FPAC-BC

(801) 844-2905

Paul Fukuhara, Project Manager, FPAC-BC

(817) 509-3395

Reviewing Official

James Flickinger

Associate Chief Information Security Officer – FPAC-BC

United States Department of Agriculture

816-926-6010

Abstract

The Geospatial Systems application is a system of the FPAC Natural Resources Conservation Service (NRCS).
The Geospatial Systems (**GS**) consolidates within the same accreditation boundary based on system functions and mission purposes. The GS includes Geospatial Data Gateway (**GDG**), Geospatial Data Warehouse (**GDW**), Geospatial Services (**GSS**), GeoObserver for Easements (**GOE**), High Resolution Elevation Data Application (**HREA**), and GeoObserver for Dams (**DAMS**).
A Privacy Threshold Analysis (PTA) was performed, indicating that a PIA must be completed. This PIA is being conducted to comply with the Federal Information Security Modernization Act of 2014 (FISMA) (44 U.S.C. §3551 to §3559) and the E-Government Act of 2002 (Pub. Law. 107-347, 44 U.S.C. §101).

Overview

GS is a system of the FPAC NRCS. NRCS provides private landowners with advice, guidance and technical services to carry out conservation practices. The NRCS is an agency within the USDA that has provided over 75 years of leadership in a partnership effort to help America's private landowners and managers. NRCS works with its partners to conserve their soil, water, and other natural resources by providing financial and technical assistance based on sound science and technology suited to a customer's specific needs.

The Geospatial Systems (**GS**) consolidates within the same accreditation boundary based on system functions and mission purposes. The GS includes Geospatial Data Gateway (**GDG**), Geospatial Data Warehouse (**GDW**), Geospatial Services (**GSS**), GeoObserver for Easements (**GOE**), High Resolution Elevation Data Application (**HREA**), and GeoObserver for Dams (**DAMS**).

A. Geospatial Data Warehouse

The Geospatial Data Warehouse (GDW) is the repository and support systems for storing, managing, archiving, and provisioning geospatial data for NRCS in support of NRCS programs, users, and congressional mandates. The GDW is not an application. It is a system of data stores, COTS software and provisioning/management tools for supporting geospatial data. GDW provides output to Geospatial Services, Geospatial Data Gateway, High Resolution Elevation Data Mart, and Remote Sensing Data Mart.

B. Geospatial Data Gateway

The Geospatial Data Gateway (**Gateway** or **GDG**) provides a single access point for resource data. Users can easily locate data that exist for geographic areas, find the types of data for that area, and deliver the data packaged in formats compatible with commercial and Service Center application formats. The datasets served by the gateway are outlined in the USDA Service Center Geographic Information System (**GIS**) Strategy. The public also has access to the Gateway to find and retrieve resource data.

C. GeoObserver for Dams

The GeoObserver for Dams (**DAMS**) application provides a nationally consistent workflow mechanism for NRCS National and State Engineers and Watershed Program Managers (or their designees) to review the NRCS Inventory of Dams (**NRCSID**) geodatabase, to verify or correct existing dam locations, to update dam attributes, to add new dams, and to create reports. The NRCSID dataset is maintained in a geodatabase using ArcGIS, based on the 50+ disparate Microsoft Excel spreadsheets that were previously used to manage this data locally within each state. This web-based application provides a centralized method to make updates to this NRCSID dataset.

NRCS is required to maintain an inventory of agency dams reflecting all work completed on compliance with operation and maintenance, hazard classification updates, rehabilitation and remedial activity, and status of emergency action plans on high hazard dams, along with any other changes to the NRCSID. These data must be submitted annually to the U.S. Army Corp of Engineers (USACE).

D. Geospatial Services

Geospatial Services (aka **Geo Data Services** or **GSS**) is an infrastructure component built to supply many NRCS applications with geospatial data and imagery data. Currently, GSS supports Conservation Desktop, Mobile Planner, Web Soil Survey, GeoObserver for Easements. GSS delivers geospatial data to users in the Partner Agencies and supply imagery for NRCS' in house applications as well. GSS provides geospatial data for county, state, region, or nation via ArcGIS REST services, XML and SOAP which can be used in support of conservation programs, analyzing, and reporting progress, and management applications. To do this, GeoSpatial Services publishes read only imagery data and other geospatial boundaries (roadways, rivers, state boundaries, county boundaries, etc.) inside the NRCS firewall as a web service where other applications can consume the data for their use. The applications do not log into GeoSpatial Services.

E. Remote Sensing Data Mart

The Remote Sensing Data Mart (**RSDM**) is a system for managing imagery used in support of the National Resource Inventory (**NRI**) and Stewardship Lands Imagery (**SLI**) programs.

The NRI provides natural resource managers, policy makers, scientific researchers and the public with scientifically valid, timely, and relevant information on the condition and trends of natural resources and the environment. This information provides a scientific basis for effective public policies, sound agricultural and natural resource legislation, sensible state and national conservation programs, and targeting USDA financial and technical assistance in addressing natural resource issues and concerns. Data and estimates from NRI surveys are one of the core components of the agency's strategic planning and accountability efforts and are used to assess consequences of existing legislative mandates, such as the current Farm Bill.

F. GeoObserver for Easements

GeoObserver for Easements application is to provide easements program division a way to remotely monitor the easements and prioritize their field visits based on aerial imagery observation. The application allows the users to create graphics on the screen, to store that information on a database, and to retrieve that information whenever needed. GeoObserver provides the ability to update the status of the observations based on previous agreements, additional inferences from imagery, or field observations. The information provided by the application is both spatial and tabular in nature. GeoObserver application uses Geographical Information System (GIS) tools and techniques to assist the users to monitor easements belonging to NRCS.

Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

1.1 What information is collected, used, disseminated, or maintained in the system?

GDG collects the user's contact email address.

1.2 What are the sources of the information in the system?

Information is gathered from the public users.

1.3 Why is the information being collected, used, disseminated, or maintained?

GDG: The Information collected is used for reporting purposes that includes the amount of data ordered and what domains are ordering specific products (with the number of megabytes and counts of the delivery method).

1.4 How is the information collected?

GDG collects customer order data from the customer placing orders for Geospatial data. It is collected via web-based interface, which is open to the public.

1.5 How will the information be checked for accuracy?

The GDG form includes automatic format validation of some entered user data.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

These regulations are applicable:

- Privacy Act (5 U.S.C. §552a);

- E-Government Act of 2002 (Pub. Law. 107-347, 44 U.S.C. §101); and

- Paperwork Reduction Act of 1995 (44 U.S.C. §3501).

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

- GDG collects the Contact email address of the user.
- The primary privacy risk is that sensitive personal information relative to the users could be release to unauthorized personnel. The risk is mitigated by virtue of the fact that the information gathered by GS can only be accessed by NRCS employees who are authenticated via the USDA eAuthentication (eAuth) system.
- Refer to Section 2.4 and Section 8.6 for a further discussion of security controls that are in place to mitigate privacy risks.

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Describe all the uses of information.

GDG collects the information to use to provide the customer with links to download geospatial data or for requests for support.

2.2 What types of tools are used to analyze data and what type of data may be produced?

GDG generates reports that are only available for administrators to quantify orders by sources of requests from email domains, types of data ordered, etc.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

GDG does not use commercial or publicly available data.

2.4 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

- This application is in compliance with the FISMA and the security and privacy controls provided in the U.S. National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 4.
- If any residual risks are identified, they will be managed and reported via the FISMA mandated risk assessment processes.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 How long is information retained?

- All information contained will be retained in compliance with NARA Guidelines, which vary on average in years from less than one year to more than ten years according to the NARA General Records Schedules Transmittal 29, issued December 2017.
- Per the NRCS-1 System of Record Notice (SORN), "Records are maintained as long as the owner, operator, producer, or participant qualifies for conservation programs"

3.2 Has the retention period been approved by the component records officer and the National Archives and Records Administration (NARA)?

Yes

3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

- The primary privacy risk is that a data breach could result in the release of information on members of the public. Any privacy risks are mitigated by limited access to the data by NRCS administrators and personnel, and controlled storage of the data located in controlled facilities.
- Retention of application-specific data is required to meet business and organizational requirements for this particular information system. The risks associated with retaining application-specific information are mitigated by the controls discussed above.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the United States Department of Agriculture.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

NRCS's National Geospatial Center of Excellence (NGCE) for reporting purposes, to show the amount of data ordered and what domains are ordering specific products, with the number of megabytes and counts of the delivery method.

4.2 How is the information transmitted or disclosed?

GDG generates reports that are only available for NGCE administrators to quantify orders by sources of requests from email domains, types of data ordered, etc.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Privacy risks are mitigated by ensuring that access to the data is through established security rules via eAuth. Any residual risks are mitigated by the controls discussed in Section 2.4 above.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to USDA which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

N/A- PII is not shared or disclosed with organizations that are external to the USDA.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of USDA.

- N/A- PII is not shared or disclosed with organizations that are external to the USDA.
- However, GS is subject to the NRCS-1 SORN. URL: https://www.ocio.usda.gov/sites/default/files/docs/2012/NRCS-1.txt

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

N/A- PII is not shared or disclosed with organizations that are external to the USDA.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

Privacy risks are mitigated by virtue of NOT sharing information external to the USDA. Any residual risks are mitigated by the controls discussed in Section 2.4.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Does this system require a SORN and if so, please provide SORN name and URL.

GS is subject to the NRCS-1 SORN. URL:
https://www.ocio.usda.gov/sites/default/files/docs/2012/NRCS-1.txt

6.2 Was notice provided to the individual prior to collection of information?

Yes. NRCS Privacy Policy published on the USDA website and also published on the GDG website.

6.3 Do individuals have the opportunity and/or right to decline to provide information?

Yes. Only the user's email address is necessary, should the user choose to request the data.

6.4 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

The user can choose to enter their information to provide them with links to download geospatial data or can choose to not use the system to obtain the information.

6.5 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

• Notice is provided as noted above, by the Privacy Notice on the websites and by the SORN.
• There is limited risk that the user is unaware of the collection of information, as the user is required to enter their information to obtain the information.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

7.1 What are the procedures that allow individuals to gain access to their information?

As published in SORN USDA/NRCS-1: "Any individual may request information regarding this system of records, or information as to whether the system contains records pertaining to him/her by contacting the respective district conservationist or other designee. If the specific location of the record is not known, the individual should address his/her request to the Director, Management Services Division, USDA-Natural Resources Conservation Service, P.O. Box 2890, Washington, DC 20013, who will refer it to the appropriate field office. A request for information pertaining to an individual should contain: Name, address, and other relevant information (e.g., name or nature of program, name of cooperating body, etc.)."

7.2 What are the procedures for correcting inaccurate or erroneous information?

As published in SORN USDA/NRCS-1: "Any individual may obtain information as to the procedures for contesting a record in the system which pertains to him/her by submitting a written request to the district conservationist or his/her designated representative or to the Director, Management Services Division, USDA-Natural Resources Conservation Service, P.O. Box 2890, Washington, DC 20013."

7.3 How are individuals notified of the procedures for correcting their information?

The SORN USDA/NRCS-1 is published on the USDA.gov website.

7.4 If no formal redress is provided, what alternatives are available to the individual?

N/A- See section 7.3.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

Residual privacy risks associated with the redress process for individuals are mitigated since individuals can use the relevant procedures discussed above to update their original public records.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system and are they documented?

- Users only have access to the provided public data. All PII information is protected and is only accessed by authorized NRCS staff, via USDA's Role Based Access Control (RBAC) and USDA eAuthentication.
- The application/system has documented Access Control Procedures, in compliance with FISMA and USDA directives. See Section 2.4.

8.2 Will Department contractors have access to the system?

Yes. Department contractors with a need to know will have access to this application as part of their regular assigned duties. Contractors are required to undergo mandatory background investigations commensurate with the sensitivity of their responsibilities, in compliance with Federal requirements.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

NRCS requires that every employee and contractor receives information security awareness training before being granted network and account access, which contains the requisite privacy training, and Annual Security Awareness and Specialized Training, as required by FISMA (NIST SP 800-53 rev 4) and USDA policies (USDA OCIO DR 3545-001 – Information Security Awareness and Training Policy and USDA OCIO DR 3505-003 - Access Control Policy).

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

Yes.

- ATO Initial Authorization Date: 10/1/2013
- Last Authorization Date: 12/21/2017
- Expiration Date: 12/21/2020

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

NRCS complies with the "Federal Information Security Modernization Act of 2014" (FISMA). Assessment and Accreditation, as well as annual key control self assessments, and continuous monitoring procedures are implemented for this application per the requirements given in National Institute of Standards and Technology (NIST) Special Publication 800-53,

Rev. 4. Additionally, the system provides technical safeguards to prevent misuse of data including:

- Confidentiality: Encryption is implemented to secure data at rest and in transit for this application (e.g., by FIPS 140-2 compliant HTTPS and enduser hard disk encryption).
- Integrity: Masking of applicable information is performed for this application (e.g., passwords are masked by eAuth).
- Access Control: The systems implements least privileges and need to know to control access to PII (e.g., by RBAC). Administrative and management operational controls in place to ensure proper access termination.
- Authentication: Access to the system and session timeout is implemented for this application (e.g. by eAuth and via multi-factor authentication for remote access).
- Audit: Logging is implemented for this application (e.g. by logging infrastructure).
- Attack Mitigation: The system implements security mechanisms such as input validation.

Notice: For the privacy notice control, please see Section 6 which addresses notice. For the privacy redress control, please see Section 7 which addresses redress.

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

Any privacy risks identified in this system are mitigated by the security and privacy safeguards provided in Section 8.5, and by the security controls discussed in Section 2.4 above. Remediation of privacy risks associated with internal/external sharing are addressed in PIA Sections 4 and 5, respectively.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware and other technology.

- **9.1 What type of project is the program or system?**

GS is a web-based application housed within the OCIO-NITC Data Center in Kansas City, MO.

9.2 Does the project employ technology which may raise privacy concerns? If so please discuss their implementation.

No, the project utilizes Agency approved technologies, and these technology choices do not raise privacy concerns.

Section 10.0 Third Party Websites/Applications

The following questions are directed at critically analyzing the privacy impact of using third party websites and/or applications.

10.1 Has the System Owner (SO) and/or Information Systems Security Program Manager (ISSPM) reviewed Office of Management and Budget (OMB) memorandums M-10-22 "Guidance for Online Use of Web Measurement and Customization Technology" and M-10-23 "Guidance for Agency Use of Third-Party Websites and Applications"?

Yes

10.2 What is the specific purpose of the agency's use of 3rd party websites and/or applications?

N/A - Third party websites / applications are not used.

10.3 What personally identifiable information (PII) will become available through the agency's use of 3rd party websites and/or applications.

N/A - Third party websites / applications are not used.

10.4 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be used?

N/A - Third party websites / applications are not used.

10.5 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be maintained and secured?

N/A - Third party websites / applications are not used.

10.6 Is the PII that becomes available through the agency's use of 3rd party websites and/or applications purged periodically?

N/A - Third party websites / applications are not used.

10.7 Who will have access to PII that becomes available through the agency's use of 3rd party websites and/or applications?

N/A - Third party websites / applications are not used.

10.8 With whom will the PII that becomes available through the agency's use of 3rd party websites and/or applications be shared - either internally or externally?

N/A - Third party websites / applications are not used.

10.9 Will the activities involving the PII that becomes available through the agency's use of 3rd party websites and/or applications require either the creation or modification of a system of records notice (SORN)?

N/A - Third party websites / applications are not used.

10.10 Does the system use web measurement and customization technology?

No, the system does not use web measurement and customization technology.

10.11 Does the system allow users to either decline to opt-in or decide to opt-out of all uses of web measurement and customization technology?

N/A - See section 10.10.

10.12 Privacy Impact Analysis: Given the amount and type of PII that becomes available through the agency's use of 3rd party websites and/or applications, discuss the privacy risks identified and how they were mitigated.

GS does not provide access or link to Third Party websites or applications. In addition, the system does not use web measurement or customization technology.

I have carefully assessed the Privacy Impact Assessment for the GS.

Agency Responsible Officials

JAKE ZEBELL Digitally signed by JAKE ZEBELL Date: 2020.11.04 14:52:44 -07'00'

Jake Zebell
GS Information System Owner
United States Department of Agriculture

Agency Approval Signature

LANITA THOMAS Digitally signed by LANITA THOMAS Date: 2020.11.03 13:27:47 -05'00'

Lanita Thomas
Information Systems Security Program Manager
United States Department of Agriculture

Agency Privacy Approval Signature

Digitally signed by AMBER ROSS Date: 2020.10.27 11:38:46 -05'00'

Amber Ross
FPAC Privacy Officer
United States Department of Agriculture